UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

LYNETTE ARMSTRONG, HUMARA THOMAS, and JENNIFER SCOFIELD on behalf of themselves and all others similarly situated, Plaintiff, v. **GAS SOUTH, LLC** Defendant.	Case No.

CLASS ACTION COMPLAINT

Plaintiffs, Lynette Armstrong, Humara Thomas, Jennifer Scofield, individually and on behalf of the Classes defined below of similarly situated persons ("Plaintiffs"), allege the following against Gas South, LLC ("Gas South" or "Defendant") based upon personal knowledge with respect to themselves and on information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters:

INTRODUCTION

1. Plaintiffs bring this class action against Gas South for its failure to properly secure and safeguard Plaintiffs' and other similarly situated Gas South customers' Social Security numbers, driver's license numbers, bank or credit card account numbers, or other sensitive records from hackers.

2. Gas South, based in Atlanta, is a natural gas provider that serves more than 425,000 residential, commercial, and governmental customers in Georgia, Florida, North Carolina, South Carolina, New Jersey and Ohio.

3. On or about July 15, 2022, Gas South filed official notice of a hacking incident with the Montana Department of Justice. Under state law, organizations must report breaches involving Social Security numbers, driver's license numbers, bank or credit card account numbers, or medical records.

4. On or about the same day, Gas South also sent out data breach letters to individuals whose information was compromised as a result of the recent data security incident.

5. Based on the Notice filed by the company, on February 21, 2022, Gas South detected unusual activity on some of its computer systems. In response, the company disconnected the affected systems, secured its network, and commenced an investigation into the incident. The Gas South investigation revealed that an

unauthorized party had access to certain company files between February 13, 2022 and February 23, 2022 (the "Data Breach"). Yet, Gas South waited five months to notify the public that they were at risk.

6. As a result of this delayed response, Plaintiffs and Class Members had no idea for months that their Private Information had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

7. Information compromised in the Data Breach included highly sensitive data that represents a gold mine for data thieves. This includes current and former customer names, dates of birth, social security numbers, driver's license or state identification card numbers (collectively the "Private Information") and additional personally identifiable information ("PII") that Gas South collected and maintained.

8. Armed with the Private Information accessed in the Data Breach, and a four month head start, data thieves can commit a variety of crimes including, e.g., opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' information to obtain government benefits, filing fraudulent

tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

9. Therefore, Plaintiffs and Class Members will show that they have suffered ascertainable losses in the form of the loss of the benefit of their bargain, out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

10. Plaintiffs bring this class action lawsuit to address Gas South's inadequate safeguarding of Class Members' Private Information that it collected and maintained, and for failing to provide timely and adequate notice to Plaintiffs and Class Members that their information had been subject to the unauthorized access and precisely what specific type of information was accessed.

11. The potential for improper disclosure of Plaintiffs' and Class Members' Private Information was a known risk to Gas South, and thus Gas South was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

12. Gas South and its employees failed to properly monitor the computer network and systems that housed the Private Information. Had Gas South properly monitored its networks, it would have discovered the breach sooner.

13. Plaintiffs' and Class Members' identities are now at risk because of Gas South's negligent conduct since the Private Information that Gas South collected and maintained is now likely in the hands of data thieves and unauthorized third-parties.

14. Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed and/or compromised during the Data Breach.

15. Plaintiffs seek remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Gas South's data security systems, future annual audits, and adequate credit monitoring services funded by Gas South.

PARTIES

16. Plaintiff Lynette Armstrong, is, and at all times mentioned herein was, an individual citizen of the State of Georgia residing in the City of Griffin in Spalding County.

17. Plaintiff Humara Thomas, is, and at all times mentioned herein was, an individual citizen of the State of Georgia residing in the City of Hampton in Henry County.

18. Plaintiff Jennifer Scofield, is, and at all times mentioned herein was, an individual citizen of the State of New Jersey residing in the Township of Neptune in Monmouth County.

19. Defendant Gas South LLC is a natural gas provider with its principal place of business at 3625 Cumberland Blvd SE, Suite 1100, Atlanta, GA 30339 in Cobb County.

JURISDICTION AND VENUE

20. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Upon information and belief, the number of class members is over 100, many of whom have different citizenship from Defendant Gas South. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

21. This Court has jurisdiction over each of the Defendant because it operates and/or are incorporated in this District, and the computer systems implicated in this Data Breach are likely based in this District.

22. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District. Gas South has harmed to Class Members residing in this District.

GAS SOUTH COLLECTS HIGHLY SENSTIVE CUSTOMER INFORMATION

23. Gas South, LLC is a natural gas provider based in Atlanta, Georgia. Founded in 2006, Gas South quickly grew to be one of the largest natural gas companies in the southeastern United States, serving more than 425,000 customers in Georgia and 13 other states. Gas South is a wholly owned subsidiary of Cobb Electric Membership Corporation. Gas South employs more than 250 people and generates approximately $193 million in annual revenue.

24. As a condition of receiving natural gas services, Gas South requires that its customers entrust it with highly sensitive personal information. In the ordinary course of receiving service from Gas South, customers are required to provide sensitive personal and private information such as:

- Names;
- Dates of birth;
- Social Security numbers;
- Driver's license numbers and information;
- Financial account information; and
- Payment card information.

25. Gas South uses this information, *inter alia*, to perform a credit check on its customers in order to determine that customer's rate per therm of natural gas, deposit requirement, and monthly service fee.

26. In its privacy policy, Gas South promises its customers that it will not share this Personal Information with third parties:

> We do not sell your name or other private profile information to third parties, and do not intend to do so in the future. We may routinely share your information with our partners and other affiliates. From time to time, we may engage third parties to process information on our behalf; however, Gas South requires that these third parties comply with Gas South's privacy policies when processing this information. The information Gas South provides to third party vendors will be used solely as defined in each specific vendor's contract and will not be disseminated to outside parties unless agreed to in writing by both Gas South and the respective third party, or such third party provides consent via Gas South's website indicating his or her interest in receiving product or services information from related and/or unrelated third party.[1]

27. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Gas South assumed legal and equitable duties and knew or should have known, based, *inter alia*, on the prior data breach and settlement, that it was responsible for protecting Plaintiffs' and Class Members' Private Information from disclosure.

[1] https://www.gassouth.com/common/privacy-policy

28. Plaintiffs and the Class Members have taken reasonable steps to maintain the confidentiality of their Private Information.

29. Plaintiffs and the Class Members relied on Gas South to keep their Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

GAS SOUTH'S DATA BREACH AND NOTICE TO PLAINTIFFS

30. Plaintiffs were customers of Gas South. As a mandatory part of the new customer intake, Gas South collected financial information, credit report information, and driver's license information for Plaintiffs.

31. According to the company, in February 2022, Gas South learned of unauthorized access to its computer systems between February 13, 2022 and February 23, 2022. The unauthorized individual or individuals accessed a cache of highly sensitive PII, including names and social security numbers.

32. On or about July 15, 2022, about 5 months after Gas South learned that the Class's Personal Information was first accessed by cybercriminals, Gas South finally began to notify customers that its investigation identified that their Personal Information was breached. Although Gas South has not divulged to Plaintiffs, the Class, or the public the exact information that was accessed, upon

information and belief it includes or may include: an individuals' name; address and other contact information; Social Security number, date of birth, and/or driver's license number.

33. Gas South delivered Data Breach Notification Letters to Plaintiffs and the Class Members, alerting them that their highly sensitive PII had been exposed in a "Data Security Incident."

34. The notice letter then attached several pages entitled "Additional Steps You Can Take to Protect Information of an Adult" and "Additional Steps You Can Take to Protect Information of a Minor," which listed generic steps that victims of data security incidents can take, such as getting a copy of a credit report or notifying law enforcement about suspicious financial account activity. Other than providing a call center number that victims could contact "with any questions," Gas South offered no other substantive steps to help victims like Plaintiffs and the Class Members to protect themselves.

35. On information and belief, Gas South sent a similar generic letter to all individuals affected

36. Gas South had obligations created by contract, industry standards, common law, and representations made to Plaintiffs and Class Members to keep

their Private Information confidential and to protect it from unauthorized access and disclosure.

37. Plaintiffs and Class Members provided their Private Information to Gas South with the reasonable expectation and mutual understanding that Gas South would comply with its obligations to keep such information confidential and secure from unauthorized access and to provide timely notice of security breaches.

38. Gas South's data security obligations were particularly important given the substantial increase in cyberattacks.

39. Gas South knew or should have known that its electronic records would be targeted by cybercriminals.

GAS SOUTH FAILED TO COMPLY WITH FTC GUIDELINES

40. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making.

41. In October 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that

is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

42. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

43. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

44. On information and belief, Gas South failed to properly implement basic data security practices. Gas South's failure to employ reasonable and appropriate measures to protect against unauthorized access to patient PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

45. Gas South was at all times fully aware of its obligation to protect the PII of its customers.

GAS SOUTH FAILED TO COMPLY WITH INDUSTRY STANDARDS

46. As noted above, experts studying cyber security routinely identify businesses as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

47. Several best practices have been identified that a minimum should be implemented by businesses like Gas South, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data, and; limiting which employees can access sensitive data. Defendant failed to follow these industry best practices, including a failure to implement multi-factor authentication.

48. Other best cybersecurity practices that are standard in the industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points. Defendant failed to follow these cybersecurity best practices, including failure to train staff.

49. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

50. Defendant failed to comply with these accepted standards, thereby opening the door to the cyber incident and causing the data breach.

GAS SOUTH'S SECURITY OBLIGATIONS

51. Gas South breached its obligations to Plaintiffs and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain

and safeguard its computer systems and data. Gas South's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect customers' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to sufficiently train its employees in the proper handling of emails containing PII;

e. Failing to fully comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act, and;

f. Failing to adhere to industry standards for cybersecurity.

52. As the result of computer systems in need of security upgrading, inadequate procedures for handling emails containing viruses or other malignant computer code, and employees who opened files containing the virus or malignant code that perpetrated the cyberattack, Gas South negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information.

53. Accordingly, as outlined below, Plaintiffs' and Class Members' daily lives were severely disrupted. What's more, they now face an increased risk of

fraud and identity theft. Plaintiffs and the Class Members also lost the benefit of the bargain they made with Gas South.

DATA BREACHES, FRAUD AND IDENTITY THEFT

54. The FTC hosted a workshop to discuss "informational injuries" which are injuries that consumers suffer from privacy and security incidents, such as data breaches or unauthorized disclosure of data.[2] Exposure of personal information that a consumer wishes to keep private, may cause both market and non-market harm to the consumer, such as the ability to obtain or keep employment. Consumers loss of trust in e-commerce also deprives them of the benefits provided by the full range of goods and services available which can have negative impacts on daily life.

55. Any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, or take over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to

[2] *FTC Information Injury Workshop, BE and BCP Staff Perspective*, Federal Trade Commission, (October 2018), *available at* https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_staff_report_-_oct_2018_0.pdf.

take on the victim's identity, or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

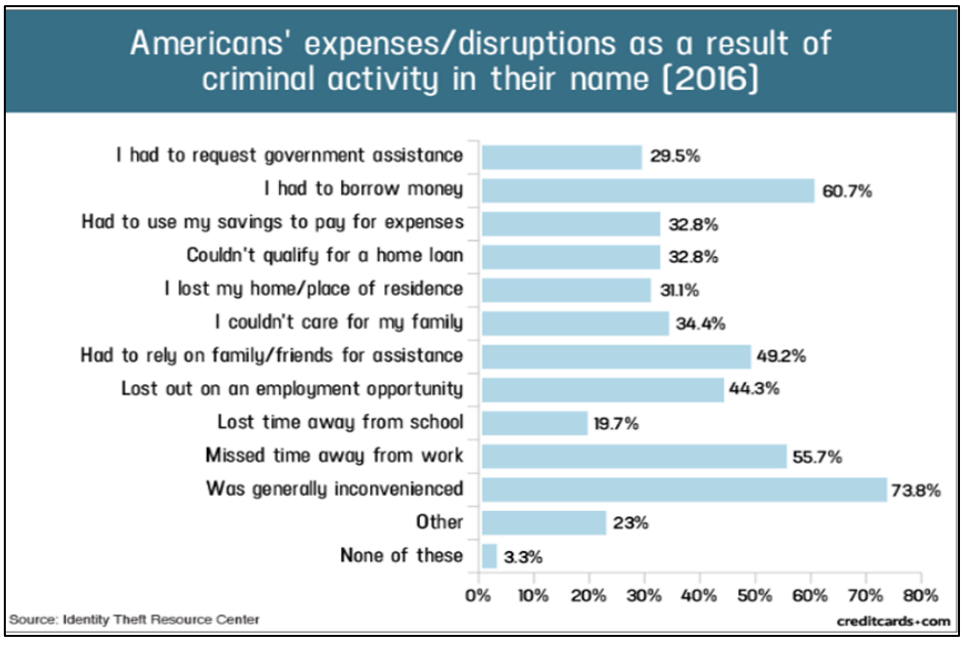
56. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[3]

57. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

[3] *See IdentityTheft.gov*, Federal Trade Commission, *available at* https://www.identitytheft.gov/Steps (last visited August 11, 2022).

58. Identity thieves can also use Social Security numbers and driver's license numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

59. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of PII:[4]



[4] Steele, Jason, *Credit Card and ID Theft Statistics*, CreditCards.com (October 23, 2017), *available at* https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276/.

60. Moreover, theft of Private Information is also gravely serious. Its value is axiomatic, considering the value of "big data" in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

61. It must also be noted there may be a substantial time lag – measured in years -- between when harm occurs and when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:[5]

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

62. Private Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black market" for years.

[5] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO (June 2007), *available at* https://www.gao.gov/assets/270/262904.html.

63. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiffs and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

PLAINTIFFS AND CLASS MEMBERS' DAMAGES

64. Plaintiffs and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

65. Plaintiffs' Private Information, including her sensitive PII, was compromised as a direct and proximate result of the Data Breach.

66. As a direct and proximate result of Gas South's conduct, Plaintiffs and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

67. As a direct and proximate result of Gas South's conduct, Plaintiffs and Class Members have been forced to expend time dealing with the effects of the Data Breach.

68. Plaintiffs and Class Members face substantial risk of out-of-pocket fraud losses such as medical services billed in their names, loans opened in their

names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

69. Plaintiffs and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to target such schemes more effectively to Plaintiffs and Class Members.

70. Plaintiffs and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

71. The information that Gas South maintains regarding Plaintiffs and Class Members, when combined with publicly available information, would allow nefarious actors to paint a complete financial and personal history of Plaintiffs and Class Members.

72. Plaintiffs and Class Members were also damaged via benefit-of-the-bargain damages. Plaintiffs and Class Members overpaid for a service that was intended to be accompanied by adequate data security but was not. Part of the price Plaintiffs and Class Members paid to Gas South was intended to be used by Gas South to fund adequate security of Gas South's computer property and protect

Plaintiffs' and Class Members' Private Information. Thus, Plaintiffs and the Class Members did not get what they paid for.

73. Plaintiffs and Class Members have spent and will continue to spend significant amounts of time to monitor their financial and medical accounts and records for misuse.

74. Plaintiffs and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Finding fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Purchasing credit monitoring and identity theft prevention;

d. Addressing their inability to withdraw funds linked to compromised accounts;

e. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

f. Placing "freezes" and "alerts" with credit reporting agencies;

g. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

h. Contacting financial institutions and closing or modifying financial accounts;

i. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

j. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled, and;

k. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

75. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Gas South, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing personal and financial information is not accessible online, that access to such data is password-protected, and that such data is properly encrypted.

76. As a direct and proximate result of Gas South's actions and inactions, Plaintiffs and Class Members have suffered a loss of privacy and either have suffered harm or are at an imminent and increased risk of future harm.

CLASS ALLEGATIONS

77. Plaintiffs bring this action pursuant to Rule 23 of the Federal Rules of Civil Procedure on behalf of themselves and on behalf of all other persons similarly situated (the "Class").

78. Plaintiffs propose the following Class definitions, subject to amendment as appropriate:

> **Nationwide Class**
>
> All individuals in the United States who had Private Information stolen as a result of the Data Breach, including all who were sent a notice of the Data Breach.
>
> **Georgia Subclass**
>
> All residents of Georgia who had Private Information stolen as a result of the Data Breach, including all who were sent a notice of the Data Breach.
>
> **New Jersey Subclass**
>
> All residents of New Jersey who had Private Information stolen as a result of the Data Breach, including all who were sent a notice of the Data Breach.

79. Excluded from each of the above Classes are Defendant and its parents or subsidiaries, any entities in which it has a controlling interest, as well as their officers, directors, affiliates, legal representatives, heirs, predecessors,

successors, and assigns. Also excluded are any Judge to whom this case is assigned as well as his or her judicial staff and immediate family members.

80. Plaintiffs reserve the right to modify or amend the definitions of the proposed Classes before the Court determines whether certification is appropriate.

81. Each of the proposed classes meet the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3).

82. Numerosity**.** The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time, based on information and belief, the Class consists of thousands of customers of Gas South whose data was compromised in the Data Breach. The identities of Class Members are ascertainable through Gas South's records, Class Members' records, publication notice, self-identification, and other means.

83. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Gas South engaged in the conduct alleged herein;

b. Whether Gas South's conduct violated the Georgia Deceptive Trade Practices Act, invoked below;

c. When Gas South actually learned of the data breach and whether its response was adequate;

d. Whether Gas South unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' Private Information;

e. Whether Gas South failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

f. Whether Gas South's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

g. Whether Gas South's data security systems prior to and during the Data Breach were consistent with industry standards;

h. Whether Gas South owed a duty to Class Members to safeguard their Private Information;

i. Whether Gas South breached its duty to Class Members to safeguard their Private Information;

j. Whether computer hackers obtained Class Members' Private Information in the Data Breach;

k. Whether Gas South had a legal duty to provide timely and accurate notice of the data breach to Plaintiffs and the Class Members;

l. Whether Gas South breached its duty to provide timely and accurate notice of the data breach to Plaintiffs and the Class Members;

m. Whether Gas South knew or should have known that its data security systems and monitoring processes were deficient;

n. What damages Plaintiffs and Class Members suffered as a result of Gas South's misconduct;

o. Whether Gas South's conduct was negligent;

p. Whether Gas South's conduct was *per se* negligent;

q. Whether Gas South was unjustly enriched;

r. Whether Plaintiffs and Class Members are entitled to actual and/or statutory damages;

s. Whether Plaintiffs and the other Class Members are entitled to additional credit or identity monitoring and are entitled to other monetary relief; and

t. Whether Plaintiffs and the Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

84. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' Private Information, like that of every other Class Member, was compromised in the Data Breach.

85. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiffs' Counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

86. Predominance**.** Gas South has engaged in a common course of conduct toward Plaintiffs and Class Members, in that all the Plaintiffs' and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Gas South's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

87. Superiority**.** A Class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common

questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Gas South. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

88. Class certification also is appropriate under Fed. R. Civ. P. 23(b)(2). Gas South has acted or has refused to act on grounds generally applicable to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

89. Finally, all members of the proposed Class are readily ascertainable. Gas South has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Gas South.

CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS OR ALTERNATIVELY THE GEORGIA AND NEW JERSEY SUBCLASSES)

90. Plaintiffs restate and reallege all proceeding allegations above and hereafter as if fully set forth herein.

91. Gas South knowingly collected, came into possession of, and maintained Plaintiffs' and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

92. Gas South's duty included a responsibility to implement processes by which they could detect and analyze a breach of its security systems in an expeditious period of time and to give prompt notice to those affected in the case of a cyberattack.

93. Gas South knew, or should have known, of the risks inherent in collecting the Private Information of Plaintiffs and the Class Members and the importance of adequate security. Gas South was on notice because on information

and belief it knew or should have known that utility entities are an attractive target for cyberattacks.

94. Gas South owed a duty of care to Plaintiffs and the Class Members whose Private Information was entrusted to it. Gas South's duties included, but were not limited to, the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting Private Information in its possession;

b. To protect customers' Private Information using reasonable and adequate security procedures and systems that are compliant with the industry standards;

c. To have procedures in place to prevent the loss or unauthorized dissemination of Private Information in its possession;

d. To employ reasonable security measures and otherwise protect the Private Information of Plaintiffs and Class Members pursuant to the Georgia Fair Business Practices Act;

e. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches, and

f. To promptly notify Plaintiffs and the Class Members of the data breach, and to disclose precisely the type(s) of information compromised.

95. Gas South's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant was bound by industry standards to protect confidential Personal Information.

96. Plaintiffs and the Class Members were foreseeable and probable victims of any inadequate security practices, and Gas South owed them a duty of care not to subject them to an unreasonable risk of harm.

97. Gas South, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and Class members by failing to exercise reasonable care in protecting and safeguarding Plaintiffs' and Class Members' Private Information within Gas South's possession.

98. Gas South, by its actions and/or omissions, breached its duty of care by failing to provide, or by acting with reckless disregard for, fair, reasonable, or adequate computer systems and data security practices to safeguard the Private Information of Plaintiffs and the Class Members.

99. Gas South, by its actions and/or omissions, breached its duty of care by failing to promptly identify the Data Breach and then provide prompt notice of the Data Breach to the persons whose Private Information was compromised.

100. Gas South breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of its networks and systems;

c. Failure to periodically ensure that its email system had plans in place to maintain reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' Private Information;

e. Failing to detect in a timely manner that Class Members' Private Information had been compromised; and

f. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

101. Gas South acted with reckless disregard for the rights of Plaintiffs and the Class Members by failing to provide prompt and adequate individual notice of the data breach so that they could take measures to protect themselves from damages caused by the fraudulent use of the Private Information compromised in the data breach.

102. Gas South had a special relationship with Plaintiffs and the Class Members. Plaintiffs' and the Class Members' willingness to entrust Gas South with their Private Information was predicated on the understanding that Gas South would take adequate security precautions. Moreover, only Gas South had the ability to protect its systems (and the Private Information that it stored on them) from attack.

103. Gas South's breach of duties owed to Plaintiffs and Class Members caused Plaintiffs' and Class Members' Private Information to be compromised.

104. As a result of Gas South's ongoing failure to notify Plaintiffs and Class Members regarding exactly what Private Information has been compromised,

Plaintiffs and Class Members are unable to take all the necessary precautions to mitigate damages by preventing future fraud.

105. Gas South's breaches of duty caused a foreseeable risk of harm to Plaintiffs and Class Members to suffer from identity theft, loss of time and money to monitor their finances for fraud, and loss of control over their Private Information.

106. As a result of Gas South's negligence and breach of duties, Plaintiffs and Class Members are in danger of imminent harm in that their Private Information, which is still in the possession of third parties, will be used for fraudulent purposes.

107. Gas South also had independent duties under state laws that required it to reasonably safeguard Plaintiffs' and the Class Members' Private Information and promptly notify them about the data breach.

108. As a direct and proximate result of Gas South's negligent conduct, Plaintiffs and the Class Members have suffered damages and are at imminent risk of further harm.

109. The injury and harm that Plaintiffs and the Class Members suffered (as alleged above) was reasonably foreseeable.

110. The injury and harm that Plaintiffs and the Class Members suffered (as alleged above) was the direct and proximate result of Gas South's negligent conduct.

111. Plaintiffs and the Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

112. In addition to monetary relief, Plaintiffs and the Class Members also are entitled to injunctive relief requiring Gas South to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and the Class Members.

COUNT II
NEGLIGENCE *PER SE*
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS OR ALTERNATIVELY THE GEORGIA AND NEWJERSEY SUBCLASSES)

113. Plaintiffs restate and reallege the allegations in paragraphs 1-89 as if fully set forth herein.

114. Pursuant to Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, Gas South had a duty to provide fair and adequate computer systems and data security to safeguard the Private Information, including PII, of Plaintiffs and the Class Members.

115. Gas South breached its duties by failing to employ industry standard data and cybersecurity measures to gain compliance with those laws, including, but not limited to, proper segregation, access controls, password protection, encryption, intrusion detection, secure destruction of unnecessary data, and penetration testing.

116. Plaintiffs and the Class Members are within the class of persons that the FTCA is intended to protect.

117. The FTCA prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice of failing to use reasonable measures to protect Private Information. The FTC publications described above, and the industry standard data and cybersecurity measures, also form part of the basis of Gas South's duty in this regard.

118. Gas South violated the FTCA by failing to use reasonable measures to protect Private Information of Plaintiffs and the Class and not complying with applicable industry standards, as described herein.

119. It was reasonably foreseeable, particularly given the growing number of data breaches of Private Information, that the failure to reasonably protect and secure Plaintiff's and Class Members' Personal Information in compliance with applicable laws would result in an unauthorized third-party gaining access to Gas

South's networks, databases, and computers that stored or contained Plaintiff's and Class Members' Personal Information.

120. Gas South's violations of the FTCA constitutes negligence *per se*.

121. Plaintiffs' and Class Members' Private Information constitutes personal property that was stolen due to Gas South's negligence, resulting in harm, injury and damages to Plaintiffs and Class Members.

122. As a direct and proximate result of Gas South's negligence *per se*, Plaintiffs and the Class have suffered, and continue to suffer, injuries and damages arising from the unauthorized access of their Private Information, including PII, as a result of the data breach including but not limited to damages from lost time and effort to mitigate the actual and potential impact of the data breach on their lives.

123. Gas South breached its duties to Plaintiffs and the Class under these laws by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and the Class Members' Private Information.

124. As a direct and proximate result of Gas South's negligent conduct, Plaintiffs and the Class Members have suffered injury and are entitled to compensatory and consequential damages in an amount to be proven at trial.

125. In addition to monetary relief, Plaintiffs and the Class Members also are entitled to injunctive relief requiring Gas South to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and the Class Members.

COUNT III
BREACH OF CONTRACT
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS OR ALTERNATIVELY THE GEORGIA AND NEW JERSEY SUBCLASSES)

126. Plaintiffs restate and reallege the allegations in paragraphs 1-89 as if fully set forth herein.

127. Plaintiffs and Class Members entered into a valid and enforceable contract when they paid money to Gas South in exchange for services, which included promises to secure, safeguard, protect, keep private, and not disclose Plaintiffs' and Class Members' Private Information.

128. Gas South's Privacy Policy memorialized the rights and obligations of Gas South and its customers. This document was provided to Plaintiffs in a manner and during a time where it became part of the agreement for services.

129. In the Privacy Policy, Gas South commits to protecting the privacy and security of private information and promises to never share customer information except under certain limited circumstances.

130. Plaintiffs and the Class Members fully performed their obligations under their contracts with Gas South.

131. Gas South did not secure, safeguard, protect, and/or keep private Plaintiff' and Class Members' PII and/or it disclosed their PII to third parties, and therefore Gas South breached its contract with Plaintiffs and Class Members.

132. Gas South allowed third parties to access, copy, and/or transfer Plaintiffs' and Class Members' PII, without permission, and therefore Gas South breached the Privacy Policy with Plaintiffs and Class Members.

133. Gas South's failure to satisfy its confidentiality and privacy obligations resulted in Gas South providing services to Plaintiffs and Class Members that were of a diminished value.

134. As a result, Plaintiffs and Class Members have been harmed, damaged, and/or injured as described herein.

135. In addition to monetary relief, Plaintiffs and the Class Members also are entitled to injunctive relief requiring Gas South to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those

systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and the Class Members.

COUNT IV
BREACH OF IMPLIED CONTRACT
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS OR ALTERNATIVELY THE GEORGIA AND NEW JERSEY SUBCLASSES)

136. Plaintiffs restate and reallege the allegations in paragraphs 1-89 as if fully set forth herein.

137. This Count is plead in the alternative to Count III above.

138. Gas South provides natural gas services to Plaintiffs and Class Members. Plaintiffs and Class Members also formed an implied contract with Defendant regarding the provision of those services through their collective conduct, including by Plaintiff and Class Members paying for services and/or receiving pay for labor or goods from Defendant.

139. Through Defendant's performance of, sale of, and/or purchase of goods and services, it knew or should have known that it must protect Plaintiffs' and Class Members' confidential Private Information in accordance with Gas South's policies, practices, and applicable law.

140. As consideration, Plaintiffs and Class Members paid money to Gas South for natural gas services, or and turned over valuable PII to Defendant.

Accordingly, Plaintiff and Class Members bargained with Gas South to securely maintain and store their Personal Information.

141. Gas South violated these contracts by failing to employ reasonable and adequate security measures to secure Plaintiffs' and Class Members' Personal Information and by disclosing it for purposes not required or permitted under the contracts or agreements.

142. Plaintiffs and Class Members have been damaged by Gas South's conduct, including by paying for data and cybersecurity protection that they did not receive, as well as by incurring the harms and injuries arising from the Data Breach now and in the future.

COUNT V
VIOLATION OF GEORGIA UNIFORM DECEPTIVE TRADE PRACTICES ACT GEORGIA CODE ANN. §§ 10-1-370, *ET SEQ.*
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS)

143. Plaintiffs restate and reallege the allegations in paragraphs 1-89 as if fully set forth herein.

144. As fully alleged above, Defendant engaged in unfair and deceptive acts and practices in violation of the Georgia Uniform Deceptive Trade Practices Act (Ga. Code Ann., §§ 10-1-370, *et seq*.).

145. Reasonable individuals would be misled by Defendant's misrepresentations and/or omissions concerning the security of their PII, because they assume companies that collect PII from customers will properly safeguard that PII in a manner consistent with industry standards and practices.

146. Defendant did not inform customers that it failed to properly safeguard their Private Information, thus misleading Plaintiffs and Class members in violation of §10-1-370, *et seq*. Such misrepresentation was material because Plaintiff and Class members entrusted Defendant with their Personal Information.

147. Had Plaintiffs and Class members known of Defendant's failure to maintain adequate security measures to protect their Private Information, Plaintiffs and Class members would not have entrusted their Personal Information to Defendant.

148. Plaintiffs and Class Members were injured because: a) they would not have paid for services from Gas South had they known the true nature and character of Gas South's data security practices; b) Plaintiffs and Class Members would not have entrusted their Private Information to Gas South in the absence of promises that Gas South would keep their information reasonably secure, and c) Plaintiffs and Class Members would not have entrusted their Private Information to

Gas South in the absence of the promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

149. As a result, Plaintiffs and the Class Members have been damaged in an amount to be proven at trial.

150. On behalf of themselves and other members of the Class, Plaintiffs seek to enjoin the unlawful acts and practices described herein, to recover his actual damages, three times actual damages, and reasonable attorneys' fees.

COUNT VI
INTRUSION UPON SECLUSION / INVASION OF PRIVACY
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS OR ALTERNATIVELY THE GEORGIA AND NEW JERSEY SUBCLASSES)

151. Plaintiffs restate and reallege the allegations in paragraphs 1-89 as if fully set forth herein.

152. Plaintiffs and Class Members maintain a privacy interest in their Private Information, which is private, confidential information that is also protected from disclosure by applicable laws set forth above.

153. Plaintiffs and Class Members' Private Information was contained, stored, and managed electronically in Gas South's records, computers, and databases that was intended to be secured from unauthorized access to third-parties because it contained highly sensitive, confidential matters regarding Plaintiffs' and

Class Members' identities that were only shared with Gas South for the limited purpose of obtaining and paying for natural gas services.

154. Additionally, Plaintiffs' and Class Members' Private Information, when contained in electronic form, is highly attractive to criminals who can nefariously use their Private Information for fraud, identity theft, and other crimes without their knowledge and consent.

155. Gas South's disclosure of Plaintiffs' and Class Members' Private Information to unauthorized third parties as a result of its failure to adequately secure and safeguard their Private Information is offensive to a reasonable person. Gas South's disclosure of Plaintiffs' and Class Members' Private Information to unauthorized third parties permitted the physical and electronic intrusion into Plaintiffs' and Class Members' private quarters where their Private Information was stored.

156. Plaintiffs and Class Members have been damaged by Gas South's conduct, including by paying for data and cybersecurity protection that they did not receive, as well as by incurring the harms and injuries arising from the Data Breach now and in the future.

COUNT VII
UNJUST ENRICHMENT
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS OR ALTERNATIVELY THE GEORGIA AND NEW JERSEY SUBCLASS)

157. Plaintiffs restate and reallege the allegations in paragraphs 1-89 as if fully set forth herein.

158. This count is plead in the alternative to Count III above.

159. Plaintiff and Class Members conferred a benefit on Gas South by paying for products and services that should have included data and cybersecurity protection to protect their Personal Information, which was not provided and Plaintiff and Class did not receive.

160. Gas South has retained the benefits of its unlawful conduct including the amounts received for data and cybersecurity practices that it did not provide. Due to Gas South's conduct alleged herein, it would be unjust and inequitable under the circumstances for Gas South to be permitted to retain the benefit of its wrongful conduct.

161. Plaintiffs and Class Members are entitled to full refunds, restitution and/or damages from Gas South and/or an order of this Court proportionally disgorging all profits, benefits, and other compensation obtained by Gas South from its wrongful conduct. If necessary, the establishment of a constructive trust

from which the Plaintiffs and Class Members may seek restitution or compensation may be created.

162. Plaintiffs and the Class Members may not have an adequate remedy at law against Gas South, and accordingly plead this claim for unjust enrichment in addition to or, in the alternative to, other claims pleaded herein.

COUNT VIII
DECLARATORY JUDGMENT
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS OR ALTERNATIVELY THE GEORGIA AND NEW JERSEY SUBCLASS)

163. Plaintiffs restate and reallege the allegations in paragraphs 1-89 as if fully set forth herein.

164. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statute described in this Complaint.

165. Gas South owes a duty of care to Plaintiffs and the Class Members which required it to adequately secure Private Information.

166. Gas South still possesses Private Information regarding Plaintiffs and the Class Members.

167. Plaintiffs allege that Gas South's data security measures remain inadequate. Furthermore, Plaintiffs continue to suffer injury as a result of the compromise of their Private Information and remain at imminent risk that further compromises of their Private Information will occur in the future.

168. Under its authority pursuant to the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Gas South owes a legal duty to secure customers' Private Information and to timely notify customers of a data breach under the common law and Section 5 of the FTCA;

b. Gas South's existing security measures do not comply with its explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices appropriate to the nature of the information to protect customers' Private Information; and

c. Gas South continues to breach this legal duty by failing to employ reasonable measures to secure customers' Private Information.

169. This Court also should issue corresponding prospective injunctive relief requiring Gas South to employ adequate security protocols consistent with

law and industry standards to protect customers' Private Information, including the following:

a. Order Gas South to provide lifetime credit monitoring and identity theft insurance to Plaintiffs and the Class Members.

b. Order Gas South to comply with its explicit or implicit contractual obligations and duties of care, Gas South must implement and maintain reasonable security measures, including, but not limited to:

   i. engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Gas South's systems on a periodic basis, and ordering Gas South to promptly correct any problems or issues detected by such third-party security auditors;

   ii. engaging third-party security auditors and internal personnel to run automated security monitoring;

   iii. auditing, testing, and training its security personnel regarding any new or modified procedures;

iv. segmenting its user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Gas South's systems;

v. conducting regular database scanning and securing checks;

vi. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

vii. meaningfully educating its users about the threats they face as a result of the loss of their Private Information to third parties, as well as the steps Gas South's customers must take to protect themselves.

170. If an injunction is not issued, Plaintiffs will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Gas South. The risk of another such breach is real, immediate, and substantial. If another breach at Gas South occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantifiable.

171. The hardship to Plaintiffs if an injunction does not issue exceeds the hardship to Gas South if an injunction is issued. Plaintiffs will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Gas South of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Gas South has a pre-existing legal obligation to employ such measures.

172. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing a subsequent data breach at Gas South, thus eliminating the additional injuries that would result to Plaintiffs and customers whose Private Information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and the Classes described above, seek the following relief:

a. An order certifying this action as a class action under Fed. R. Civ. P. 23, defining the classes as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiffs are proper representatives of the Classes requested herein;

b. Judgment in favor of Plaintiffs and the Class Members awarding them appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, and statutory costs;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Classes as requested herein;

d. An order instructing Gas South to purchase or provide funds for lifetime credit monitoring and identity theft insurance to Plaintiffs and the Class Members;

e. An order requiring Gas South to pay the costs involved in notifying the Class Members about the judgment and administering the claims process;

f. A judgment in favor of Plaintiffs and the Classes awarding them pre-judgment and post judgment interest, reasonable attorneys' fees, costs and expenses as allowable by law, and

g. An award of such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury on all triable issues.

DATED: September 1, 2022

Respectfully submitted,

/s/ Sean Nation
SIRI & GLIMSTAD LLP
Sean Nation (GA Bar No. 313022)
Mason A. Barney (*pro hac vice* to be filed)
Ursula Smith (*pro hac vice* to be filed)
745 5th Avenue, Suite 500
New York, New York 10151
Tel: (212) 532-1091
E: snation@sirillp.com
E: mbarney@sirillp.com
E: usmith@sirillp.com